netVigilance

**ScoutNews Team**

**26 May 2004**
**Issue #21**

Weekly ScoutNews by netVigilance

**Table of Contents**



# This Week in Review

Some time during the past two weeks McAfee started incorrectly to detecting some of SecureScout's test cases as being Trojans. SecureScout's test cases have been reconfigured so this false detection and intrusion by McAfee no longer has an effect on SecureScout. This may however still affect other security products from other vendors.

The underworld is really trying to make a statement by showing off Cisco's stolen code, and at the same time Cisco is pursuing a patent for a fix on the TCP flaw discovered earlier this year. This does make one wonder when and not if we will see Cisco in the same kind of legal suits as Microsoft, has been caught up in the past years.

Is Linux safer? Will it disrupt the established world?  Here we go again!

Finally Apple's OS X is taking shots.

Enjoy reading

# Top Security News Stories this Week

- **More details surface on Cisco's stolen code**

More details about the computer code stolen from Cisco Systems Inc. surfaced on Tuesday, including new samples of the source code and information on how the code was distributed, four days after a Russian Web site reported news of the theft and posted sample code files to support the claim.
Additional copies of Cisco code files for the Internetwork Operating System (IOS) may be circulating on the Internet, after the thief compromised a Sun Microsystems Inc. server on Cisco's network, then briefly posted a link to the source code files on a file server belonging to the University of Utrecht in the Netherlands, according to Alexander Antipov, a security expert at Positive Technologies, a security consulting company in Moscow, who was interviewed by e-mail and instant messaging service.
http://www.infoworld.com/article/04/05/18/HNfbicisco_1.html?source=rss&url=http://www.infoworld.com/article/04/05/18/HNfbicisco_1.html

- **More holes discovered in Apple OS X, cor!**

Denial is not a river in Egypt
**THE CALM** arrogance of SnApple users have that the OS X system is somehow more secure than the patchwork quilt that is Windows is taking a quiet battering over at the Full-Disclosure website.
Two posts showing how to take apart the OS X operating system have been posted in the last week using flaws that the security advisory service Secunia has rated as "extremely critical". The latest was published last night.
http://www.theinquirer.net/?article=16051

- **Cisco to patent security fix**

Cisco Systems has applied for patents on technology that it claims will fix a flaw that has recently been found in one of the most common communications protocols.
Last month, Robert Barr, an in-house patent attorney for the company, publicly acknowledged that Cisco has applied for U.S. patents on fixes to a protocol called TCP, or Transmission Control Protocol. A flaw in this protocol, which is used for sending data over the Internet, was discovered last month by security expert Paul Watson, a security specialist for industry automation company Rockwell Automation. Watson's discovery resulted in a worldwide security warning that affected many vendors' products.
http://news.com.com/Cisco+to+patent+security+fix/2100-1002_3-5216494.html?part=rss&tag=feed&subj=news

- **Open Source Users Unaffected by Sasser Worm - The Internet Keeps Going Despite Flawed Proprietary Software**

Since the 'Sasser' worm hit the Telstra BigPond network at 1AM Saturday, 1st May, Australian computer users have suffered major disruptions, with thousands of home and business users running Microsoft operating systems infected and others experiencing network congestion.
No users of the popular open source operating systems such as Linux and FreeBSD have been infected. Nor were Apple Mac OS X or Unix users. As with the 'Blaster' worm in 2003, users of many ISPs have experienced network congestion and sluggishness.
http://www.linuxpr.com/releases/6903.html

- **Do you trust this penguin?**

Does Linux have what it takes to break away from its geek roots and win mainstream appeal? William Maher takes a swim with the penguin.
For a small piece of software created by a hermit-like hacker in an Finnish bedroom, Linux's rise to fame as the World's Most Dangerous OS is nothing short of amazing.
It's hard to think of a piece of software (or any other PC technology) that has had more ammunition thrown at it. It's been called a virus, been the subject of a US$1 billion lawsuit, and described as a security risk and potential tool for terrorism. And its reputation and perceived threat to the Gates empire only seems to be growing with time. "I'm not out to destroy Microsoft," creator Linus Torvalds famously told a reporter last year. "That will just be a completely unintentional side effect."
http://www.apcmag.com/apc/v3.nsf/0/FEC56244649D3FC1CA256E75000F4E03

# New Vulnerabilities Tested in SecureScout

- **14442 NAI McAfee VirusScan Enterprise 7.1 - Virus Definitions Outdated**

Virus signatures are used to detect and repair the most recently discovered viruses.

Your definitions are older than 30 days which means that you might be vulnerable to current viruses.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

**CVE Links:** GENERIC-MAP-NOMATCH

**Reference:** http://us.mcafee.com/virusInfo/default.asp?id=recentlyDiscovered

- **14443 W32/Lovgate.ab Worms (Registry Check)**

This worm bears the following characteristics:

Drops a backdoor component
Attempts to copy itself to accessible or poorly secured remote shares, scanning contiguous IP ranges, seeking accessible IPC$ or ADMIN$ shares.
Creates a share on the victim machine (share name "MEDIA").
Mails itself, constructing message uses its own SMTP engine. Email attachment may be a ZIP archive.
Additionally, mails may be sent in reply to email messages found on the victim machine (MAPI).
Performs companion virus infection of EXE files (replacing original file with a copy of itself, and renaming original with a .ZMX extension).
Terminates processes associated with various AV and security products

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

**CVE Links:** GENERIC-MAP-NOMATCH

**Reference:** http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=125301

- **17889 phpMyFAQ 1.3.12 and prior PATH Disclosure Vulnerability**

phpMyFAQ is a multilingual, completely database-driven FAQ-system. For the time being a MySQL database (support for other databases is under development) is used to store all data, PHP 4.1.0 (or higher) is needed in order to access this data. phpMyFAQ also offers a Content Management- System, flexible multi-user support, a news-system, user-tracking, language modules, templates, extensive XML-support, PDF-support, a backup-system and an easy to use installation script."

Within phpMyFAQ an input validation problem exists which allows an attacker to disclose the install path of phpMyFAQ on the server-side scripts harddisk.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Medium**

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://secunia.com/advisories/11640/ & http://security.e-matters.de/advisories/052004.html

- **17890 phpMyFAQ 1.3.12 and prior XSS Vulnerability**

phpMyFAQ is a multilingual, completely database-driven FAQ-system. For the time being a MySQL database (support for other databases is under development) is used to store all data, PHP 4.1.0 (or higher) is needed in order to access this data. phpMyFAQ also offers a Content Management- System, flexible multi-user support, a news-system, user-tracking, language modules, templates, extensive XML-support, PDF-support, a backup-system and an easy to use installation script."

Within phpMyFAQ an input validation problem exists which allows an attacker to Cross Site Scripting attacks.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **Medium**

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://secunia.com/advisories/11640/ & http://security.e-matters.de/advisories/052004.html

- **17891 PHP-Nuke 6.X and 7.X PATH Disclosure Vulnerability**

Php-Nuke is a popular freeware content management system, written in php by Francisco Burzi. This CMS (Content Management System) is used on many thousands websites, because it's freeware, easy to install and has broad set of features.

Homepage: http://phpnuke.org

A PATH Disclosure has been reported in versions 6.x through 7.3.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Medium**

**CVE Link:** No CVE Match

**Reference:** http://secunia.com/advisories/11625/ & http://www.waraxe.us/?modname=sa&id=029 & http://www.waraxe.us/?modname=sa&id=030

- **19052 Hijack iChoose**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

**CVE Link:** No CVE Match

**Reference:** http://www.pestpatrol.com/PestInfo/i/ichoose.asp

- **19053 Hijack IEPlugin**

IEPlugin is an IE Browser Helper Object. It monitors site addresses, content entered into forms, and even local filenames browsed, and pops up advertisements when it sees a targeted keyword. It also installs a process to update itself, which will attempt to connect to its servers every minute or so, very annoying if you have auto-dial.

IEPlugin is written and distributed by InfoAge Marketing International, who also run the 123Webhost and JupiterTech hosting services. However, it seems as well as spyware, IMI are also involved in writing spam-sending software ("Godmail") and a marketing operation for pheromone pills ("Flatcash").

Alias: BHO3Lib, ExplWWW or IExpl from internal names, packed: MimarSinan [Kaspersky], TrojanDownloader.Win32.OneClickNetSearch.b, TrojanDropper.Win32.Delf.av, Win Server from its process., winobject, after the DLL containing the BHO code.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

**CVE Link:** No CVE Match

**Reference:** http://www.pestpatrol.com/PestInfo/i/ieplugin.asp

- **19054 Hijack IETray**

IETray is a search sidebar hijacker pointed at search-aide.com, implemented as an Internet Explorer Browser Helper object. When other search engines are used, it occasionally opens a pop-up alert window encouraging one to use the (now hijacked) search sidebar instead. ("For faster web searches press F9")

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

**CVE Link:** No CVE Match

**Reference:** http://www.pestpatrol.com/PestInfo/i/ietray.asp

- **19055 Hijack IGetNet**

IGetNet is a keyword-search service implemented as an IE Browser Helper Object and a process run at Windows start-up (WinStart.exe or WinStart001.exe) which writes to the Hosts file. Once this modification has occurred, every time you try to contact MSN or Netscape's search sites you are re-routed though IGetNet's servers. The IGetNet server checks to see whether your search includes a keyword they have sold to one of their advertisers, and if so,

redirects you to that site. If not they forward you to the real MSN or Netscape Search so you shouldn't notice the difference.

In addition, if IGetNet is running, and you enter auto.search.msn.com, search.netscape.com, or ieautosearch in the Address field, you will find yourself at http://www.igetnet.com

IGetNet/v4: original variant, installs files 'BHO.DLL', 'rsp.dll' and 'Winstart.exe' into the 'System' folder in the Windows folder. 'Winstart.exe', run at start-up, writes entries to the Hosts file to redirect all access to MSN or Netscape search sites through to IGetNet's servers instead. (ignkeywords.com, rspsearch.com.)
IGetNet/v5: works the same as v4, but the files are now called 'BHO001.DLL', 'rsp001.dll' and 'Winstart001.exe' and they use new class IDs internally. You can tell if you have v5 as new IE windows will show the text 'Enter Keyword or Web Address here' in the address bar.
IGetNet/v6: same as v5 but has extra files.
"IGetNet/ClearSearch" is actually misnamed, and there is no business connection between IGetNet and ClearSearch.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

**CVE Link:** No CVE Match

**Reference:** http://www.pestpatrol.com/PestInfo/i/igetnet.asp

# New Vulnerabilities found this Week

❖ Omnicron OmniHTTPD Get Request Buffer Overflow Vulnerability
Reportedly OmniHTTPD is affected by a GET request buffer overflow vulnerability. This issue is due to a failure of the application to properly validate string sizes when processing user input.

This issue could allow an attacker to execute arbitrary code with the privileges of the affected web server.
http://www.securityfocus.com/bid/10376

❖ Microsoft Internet Explorer CSS Style Sheet Memory Corruption Vulnerability
Unknown vulnerability in mshtml.dll in Microsoft Internet Explorer allows remote attackers to cause a denial of service (crash) via certain HTML document that links to a CSS document with a "float: left" class description for a form element, which may trigger a null dereference.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0484

❖ DSM Light Explorer.EXE Directory Traversal Vulnerability
DSM Light has been reported to be prone to a directory traversal vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied URI input.
This issue would allow an attacker to view arbitrary, web-readable files on the affected computer. This may aid an attacker in conducting further attacks against the vulnerable computer.
http://www.securityfocus.com/bid/10381

❖ **Multiple Perl Implementation Duplication Operator Integer Overflow Vulnerability**

This buffer overflow is limited in terms of exploitation by two factors.
One, Windows has no concept of privileged (setuid) code. So, any
exploitation would almost certainly have to be remote. Second, the buffer
overflow vulnerability occurs in a set of very limited circumstances.
Specifically, ActivePerl does some cleanup on the first command item passed
-- the filename. If the file name has no extension, ActivePerl allocates a
heap-based buffer to store the variable, to which it then concatenates
'.exe' to. For all intents and purposes, this limits exploitation to
anyone able to execute a file of his/her choice via 'system' -- a dangerous
practice anyway!
http://archives.neohapsis.com/archives/fulldisclosure/2004-05/0878.html

❖ **SGI IRIX rpc.mountd Remote Denial of Service Vulnerability**

SGI IRIX is prone to a remote denial of service vulnerability. The issue presents itself due to an unspecified error in rpc.mountd, when the process parses certain RPC requests.
SGI IRIX 6.5.24 is affected by this issue, however, it is possible that other versions of IRIX are affected as well.
http://www.securityfocus.com/bid/10372

❖ **Multiple Perl Implementation System Function Call Buffer Overflow Vulnerability**

ActiveState Perl and Perl for cygwin are both reported to be prone to a buffer overflow vulnerability.
The issue is reported to exist due to a lack of sufficient bounds checking that is performed on data that is passed to a Perl system() function call. This vulnerability may permit an attacker to influence execution flow of a vulnerable Perl script to ultimately execute arbitrary code. Arbitrary code execution will occur in the context of the user who is running the malicious Perl script.
http://www.securityfocus.com/bid/10375

❖ **CVS Client RCS Diff File Corruption Vulnerability**

The client for CVS before 1.11 allows a remote malicious CVS server to create arbitrary files using certain RCS diff files that use absolute pathnames during checkouts or updates, a different vulnerability than CAN-2004-0405.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0180

❖ **PHP-Nuke Multiple Input Validation Vulnerabilities**

PHP-Nuke is prone to multiple vulnerabilities. The issues result from insufficient sanitization of user-supplied data. An attacker can carry out cross-site scripting and path disclosure attacks.
http://phpnuke.org/modules.php?name=Downloads&d_op=viewdownload&cid=9
http://www.securityfocus.com/bid/10367

❖ **Microsoft Outlook 2003 Media File Script Execution Vulnerability**

Technical final step to 'silent delivery and installation of an
executable on the target computer, no client input other than
reading an email' this can be achieved with the highly
touted 'secure-by-default' Outlook 2003 mail client from the
craftsman known as 'Microsoft'.

Default settings of the 'gadget' are: restricted zone which means no active x controls, no scripting, no file downloads etc. This can all very easily be bypassed by simply embedding in a rich text message our OLE object, one Windows Media Player. We then point our source url to our media file which includes or now run-of -the mill 0s url flip and simply by previewing or opening the email message invoke our device known as Internet Explorer to proxy our manipulation of the recipient's machine.
http://archives.neohapsis.com/archives/bugtraq/2004-05/0165.html

**Vulnerability Resource**
Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. http://www.infosyssec.org/infosyssec/

**Thank You**
Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.

**About SecureScout**
SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.
SecureScout is a trademark of NexantiS Corporation.
netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:
Customers in America and Northern Europe contact us at info@netVigilance.com
Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net